

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 64-074582

(43)Date of publication of application : 20.03.1989

(51)Int.Cl.

G09C 1/00

(21)Application number : 62-232957

(71)Applicant : NIPPON TELEGR & TELEPH CORP  
<NTT>

(22)Date of filing : 16.09.1987

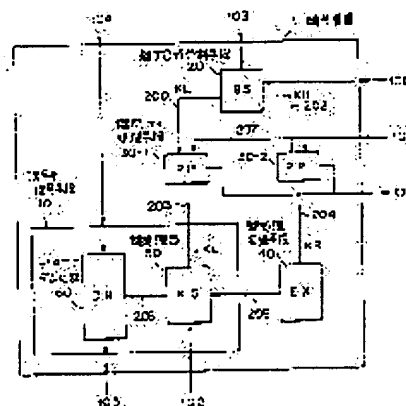
(72)Inventor : MIYAGUCHI SHOJI

## (54) CIPHERING DEVICE

### (57)Abstract:

**PURPOSE:** To attain a ciphering device having key length consisting of  $2N$  bits by a ciphering/deciphering means having key length consisting of  $N$  bits by dividing an inputted  $2N$ -bit key block into two parts, extending  $N$  bits of one divided part by a prescribed value and ciphering and deciphering the extended bits as a parameter.

**CONSTITUTION:** An input of 128 bits or the like is divided into two 64-bit key blocks KL, KR by a key block dividing means 20 in a ciphering/deciphering means 1 consisting of 64 bits or the like. The block KR transmitted through a key parity processing means 30-2 is extended to 96 bits or the like more than  $3/2 \times 64$  bits by a key processing extending means 40 and the extended block KR is supplied to a key processing part 50 in a ciphering/deciphering means 10 to which the block KR transmitted through a parity processing means 30-1 is also supplied. A normal sentence consisting of 128 bits applied to a data randomizing part 60 is ciphered by 12 parameters of 16-bit length or the like outputted from the processing part 50. Since deciphering is similarly executed, the  $2N$ -bit ciphering device can be attained by the ciphering/deciphering means having  $N$ -bit key length.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

2

⑬ 日本国特許庁(JP)

⑭ 特許出願公開

⑫ 公開特許公報(A)

昭64-74582

⑮ Int.Cl.<sup>4</sup>

識別記号

庁内整理番号

⑯ 公開 昭和64年(1989)3月20日

G 09 C 1/00

7368-5B

審査請求 未請求 発明の数 1 (全6頁)

⑰ 発明の名称 暗号装置

⑱ 特 願 昭62-232957

⑲ 出 願 昭62(1987)9月16日

⑳ 発 明 者 宮 口 庄 司 東京都千代田区内幸町1丁目1番6号 日本電信電話株式会社内

㉑ 出 願 人 日本電信電話株式会社 東京都千代田区内幸町1丁目1番6号

㉒ 代 理 人 弁理士 草 野 卓

明 細 書

1. 発明の名称

暗 号 装 置

2. 特許請求の範囲

(1) 入力された $2N$ ビットの鍵ブロックを各 $N$ ビットの鍵ブロックに分割する鍵ブロック分割手段と、

その分割された鍵ブロックの一方を $\frac{3}{2}N$ ビット以上の鍵ブロックに拡張する鍵処理拡張手段と、

その拡張された鍵ブロックをパラメータとして、上記分割された鍵ブロックとして入力し、入力データを暗号化復号処理する鍵長が $N$ ビットの暗号化復号手段とを具備する暗号装置。

3. 発明の詳細な説明

「産業上の利用分野」

この発明は、暗号鍵をパラメータとして平文から暗号文を得、及び暗号文から平文を得る暗号装置に関するものである。

「従来の技術」

従来のこの種の暗号装置は、例えば特願昭62-

37231「暗号装置」に示されている。この特許出願の第1図及び第2図を組合わせて実現される暗号装置は、暗号鍵(以降:鍵という)の長さ $N$ が64ビットである。従って、この暗号装置で得た暗号文を解読するには、鍵の全て、即ち、 $2^N = 2^{64}$ 通りの鍵について暗号文の解読を行うことができれば、暗号文は解読できる。この様な、鍵の $2^N$ 回のしらみつぶし検査は、現在のコンピュータ技術では不可能であるが、コンピュータの計算能力は年々向上しており、将来は可能となろう。このため、鍵の長さを64ビット以上に長くすることが必要であり、例えば鍵の長さ $N$ が128ビットの暗号装置が必要になると考えられる。

「問題点を解決するための手段」

この発明によれば鍵の長さ $N$ の暗号化復号手段に、小規模な鍵ブロック分割手段と鍵処理拡張手段とパリティ処理手段とを追加することにより、鍵の長さ $N$ の暗号装置と比較して極めて安全な、鍵の長さ $2N$ の暗号装置を実現する。

この発明による暗号装置は、鍵の長さが $N$ ビッ

(2)

トの暗号化復号手段に、鍵ブロック分割手段や鍵処理拡張手段等を追加することにより実現される。

この発明による暗号装置は、鍵ブロックの長さが $2N$ ビットと $N$ ビットの2種類が選択でき、選択された鍵ブロックを使って、 $m$ ビット長の平文ブロックを $m$ ビット長の暗号文に暗号化し、及び $m$ ビット長の暗号文ブロックを $m$ ビット長の平文に復号する。更に、鍵パリティ処理手段をその構成要素とする場合は、鍵ブロックの中のパリティビットの有無を指定して、 $m$ ビット長の平文ブロックを暗号化し及び $m$ ビット長の暗号文ブロックを復号する。

この発明の従来と異なる点は鍵長が $N$ ビットの暗号化復号手段を用いて、鍵長が $2N$ ビットの暗号装置が実現できる。この暗号装置は、鍵ブロックの長さが $2N$ ビットの暗号と、鍵の長さが $N$ ビットの暗号とが選択できる。

#### 「実施例1」

第1図はこの発明に基づく暗号装置1の一実施例のブロック図であり、 $N=64$ 、平文ブロック

鍵ブロック入力部であり、104はデータ入力部であり、105はデータ出力部である。信号線は、200番台の番号で図中に示す。

次に暗号装置1の各構成要素についてその機能を説明する。

#### 鍵長が $N$ ビットの暗号化復号手段10

長さが $N$ ビットの鍵ブロックを鍵パリティ処理手段30-1から入力し、暗号化復号指定入力部102で暗号化を指定した場合はデータ入力部104からの $m$ ビット(64ビット)の平文をデータ出力部105から $m$ ビット(64ビット)の暗号文として出力し、暗号化復号指定入力部102で復号を指定した場合はデータ入力部104からの $m$ ビット(64ビット)の暗号文をデータ出力部105から $m$ ビット(64ビット)の平文として出力する「鍵長が $N$ ビットのブロック暗号化復号手段」である。但し、鍵処理拡張手段40からは何も入力しない、即ち、0を入力する。

#### 鍵ブロック分割手段20

鍵ブロック長指定入力部100により鍵ブロック

や暗号文ブロック長 $m$ は、 $m=64$ の例である。

暗号装置1は鍵長が $N$ ビットの暗号化復号手段10と、鍵ブロック分割手段(BS)20と、鍵パリティ処理手段(PP)30-1及び30-2と、鍵処理拡張手段(EX)40とよりなり、鍵処理部(KS)50とデータランダム化部(DR)60とにより暗号化復号手段10が構成される。

鍵ブロック長指定入力部100は鍵ブロック長を $2N$ ビット(128ビット)とするか、または $N$ ビット(64ビット)とするかを指定する。

パリティビット有無指定入力部101は鍵ブロックの中にパリティビットが有るか、または無いかを指定する。

鍵ブロックの中にパリティビットを指定する場合は、鍵ブロックのビット位置番号 $8 \times i$ ,  $1 \leq i$ のビットとする。ここで、ブロックの中のビット位置はそのブロックの最左端ビット(MSB)から右側へ、1, 2, ...と数える。

102は暗号装置の暗号化動作、または復号動作を指定する暗号化復号指定入力部であり、103は

が128ビットと指定された場合は、鍵ブロック入力部103から入力する128ビット長の鍵ブロックを64ビットずつ2分割する。その左半分(以降KLと呼ぶ)を信号線200を介して鍵パリティ処理手段30-1へ、その右半分(以降KRと呼ぶ)を、信号線202を介して鍵パリティ処理手段30-2へそれぞれ伝える。鍵ブロックが64ビットと指定された場合は、この64ビット長の鍵ブロック(以降KLと呼ぶ)をそのまま信号線200を介して鍵パリティ処理手段30-1へ伝え、信号線202へは0を出力する。

#### 鍵パリティ処理手段30-1と30-2

第2図により説明する。鍵パリティ処理手段30-1及び30-2にそれぞれ入力した64ビットデータは、8ビットずつ8分割され部分31を通過する。このとき、8ビット長データ毎にその奇数パリティを検査するパリティ検査回路32でパリティ検査が行われ、パリティ検査結果が部分34に伝えられ、パリティビット有無指定入力部101で鍵ブロックの中にパリティ有り指定している

(3)

場合は、パリティ検査結果が出力部106により暗号装置の外部に伝えられ、パリティビット有無指定入力部101で鍵ブロックの中のパリティ無しを指定している場合は、パリティ検査結果は暗号装置の外部に伝えられない。部分31通過後の各データは、パリティビット有無指定入力部101(207)で鍵ブロックにパリティ有りを指定している場合は、第3図に示す零設定制御部33でパリティビットが零に変換される。パリティビット無しを指定している場合は、なんら変更を受けずそのまま通過する。

#### 鍵処理拡張手段 (EX) 40

第4図により説明する。入力した64ビット長のデータKRの左半分をKR0、右半分をKR1で表わす。U0は排他的論理和回路41によりKR0とKR1のビット対応の排他的論理和演算を行い、 $U0 = KR0 \oplus KR1$ 、 $U1 = KR0$ 、 $U2 = KR1$ 、等号は右辺を左辺へ代入)、信号線205へ出力する。

#### 鍵処理部 (KS) 50

( $f_k(\alpha, \beta)$ )を右データとして次段の拡散処理段54へ出力する。回路55は、初段の拡散処理段では適当な定数D0と回路52の出力を入力して、その他の拡散処理段では前段の左データと回路52の出力とを入力する。各拡散処理段54のデータ拡散手段56は、パラメータ $P_0, P_1, \dots, P_n$ を出力する。

パラメータの順序変更部57は暗号化復号指定入力部102により暗号化を指定した場合のパラメータの出力順序は、 $P_4, P_5, P_6, P_7, P_0, P_1, P_2, P_3, P_8, P_9, P_{10}, P_{11}, P_{12}, P_{13}, P_{14}, P_{15}$ であり、暗号化復号指定入力部102により復号を指定した場合のパラメータの出力順序は、 $P_8, P_9, P_{10}, P_{11}, P_{12}, P_{13}, P_{14}, P_{15}, P_4, P_5, P_6, P_7$ である。鍵処理部50から部分51を除いた部分が、特願昭62-37231の第2図の鍵処理部のブロック図に相当する部分、但し、回路52は回路51を追加するための追加改造部分である。

#### データランダム化部 (DR) 60

第6図により説明する。信号線206から入力さ

る第5図により説明する。信号線205から入力した各32ビット長のデータU0, U1, U2は、部分51内で分岐し、U0はデータのかき混ぜ処理を行う拡散処理段54の1段目と4段目の回路52へ、U1は拡散処理段54の2段目と5段目の回路52へ、U2は拡散処理段54の3段目と6段目の回路52へ入力する。ここで、回路52は、32ビット中のビット対応の排他的論理和回路である。信号線203から入力した64ビット長のデータKLは、分割回路53で32ビットずつの左データ及び右データに分割されて、複数の拡散処理段54の縦続配列の1段目(初段)に入力される。各拡散処理段54では右データは、そのまま次段の左データとして出力すると共に、回路52に供給される。32ビット中のビット対応の排他的論理和回路55は、前段の左データと回路52の出力とを入力してこれらを排他的論理和演算する。データ拡散手段56は、左データ(4)と回路55の演算結果(4)とを入力してこれらデータを混ぜ合わせるデータ拡散処理を行い、その出力

れるパラメータについては、1番目から4番目に入力されたパラメータは回路61へ供給され、5番目～8番目に入力されたパラメータは、それぞれデータ拡散手段64-1～64-4に供給され、9番目から12番目に入力されたパラメータは回路67へ供給される。データ入力部104から64ビットの入力データ(平文)が入力され、信号線206をへて供給される64ビットのパラメータ $P_4, P_5, P_6, P_7$ と排他的論理和回路61により排他的論理和演算され、その出力の左半分データと、右半分データが排他的論理和回路62で排他的論理和演算され、次にその出力はデータのかき混ぜ処理を行うデータ拡散手段64-1と、排他的論理和回路65-1との組み合わせによりデータのかき混ぜが行われ、以下同様に、データ拡散手段64-2と回路65-2によるデータかき混ぜ、データ拡散手段64-3と回路65-3によるデータかき混ぜ、データ拡散手段64-4と回路64-4によるデータかき混ぜの処理を受け、排他的論理和回路66で右半分データと左半分データの

(4)

排他的論理和演算を、排他的論理和回路67で、信号線206をへて供給される64ビットのパラメータ $P_8, P_9, P_{10}, P_{11}$ と排他的論理和演算され、その64ビットの出力がデータランダム化部60の出力(暗号文)となりデータ出力部105へ出力される。入力データとして暗号文を入力した場合は、以上述べたパラメータデータは、回路61には、 $P_8, P_9, P_{10}, P_{11}$ を、データ拡散手段64-1, 64-2, 64-3, 64-4には、 $P_3, P_2, P_0, P_1$ を、回路67には $P_4, P_5, P_6, P_7$ を入力すると、暗号文が復号された平文が105から出力される。データランダム化部60は、特願昭62-37231の第1図の暗号処理部のブロック図に相当する。

#### 暗号装置の動作

最初に鍵ブロック長指定入力部100で、鍵ブロック長を128ビットとするか64ビットとするかを指定し、パリティビット有無指定入力部101で鍵ブロックのパリティビット有無を指定し、暗号化復号指定入力部102で暗号化を行うか復号を行うかを指定する。鍵ブロックを鍵ブロック入力部

103から入力し、暗号化指定の場合はデータ入力部104から平文を、復号指定の場合はデータ入力部104から暗号文を入力する。鍵ブロックが128ビット指定の場合は、鍵ブロックが鍵ブロック分割手段20で2分され、その左半分(KL)は信号線200をへて鍵パリティ処理手段30-1へ、その右半分(KR)は信号線202をへて鍵パリティ処理手段30-2へ伝えられる。鍵ブロックの長さ64ビットを指定した場合は、入力した鍵ブロック(KL)は信号線200をへて鍵パリティ処理手段30-1へ伝えられ、信号線202へは0を出力する。信号線200上のブロック値をKL、信号線202上のブロック値をKRで表わす。鍵ブロックのパリティ無しを指定した場合は、KLは鍵パリティ処理手段30-1を、KRは鍵パリティ処理手段30-2をそのまま通過し、それぞれ信号線203または204をへて鍵処理部50または鍵処理拡張手段40へ伝えられる。鍵ブロックのパリティ有りを指定した場合は、KLとKRともそれらの全パリティビットが0に設定され、信号線

203または204をへて鍵処理部50または鍵処理拡張手段40へ伝えられる。鍵ブロックのパリティエラーの有無しの検出結果は、出力部106をへて暗号装置の外部に伝えられる。鍵処理拡張手段40に入力したKRは、鍵の拡張処理を受け96ビット長データとして信号線205をへて鍵処理部50へ伝えられる。信号線203をへて鍵処理部50に入力したデータ(KL)は、信号線205から入力された96ビット長データと一定の処理を受ける。鍵処理部50は、暗号化復号指定入力部102の暗号化または復号の指定に従い、各16ビット長の12個のパラメータ $P_i$  ( $1 \leq i \leq 16$ )を信号線206から一定順序で出力する。データランダム化部60はデータ入力部104からの入力データ(平文または暗号文)を、信号線206からのパラメータを受け入れて一定の処理を行い、データ出力部105から出力データ(暗号文または平文)を出力する。

以上述べた暗号装置の動作を、数式を用いて再度説明する。

ブロック $B_1, B_2, \dots$ をこの順序にならべてできるブロック、即ち、 $B_1, B_2, \dots$ の連結を、( $B_1, B_2, \dots$ )で表わす。 $\oplus$ は、ブロック間のビット対応の排他的論理和演算を表わす。例えば、 $B_1 = 00001111, B_2 = 00111100$  のとき、 $B_1 \oplus B_2 = 00110011$ である。等号 $=$ は、右辺を左辺に代入することを表わす。

(鍵ブロック分割手段20の処理)

KL, KRは64ビット長ブロックを表わす変数とする。鍵ブロック長が128ビットを指定した場合は、入力した鍵を64ビットずつ2分し、KL=鍵の左半分、KR=鍵の右半分とする。鍵ブロック長=64ビットを指定した場合は、KL=入力した鍵、KR=0とする。

(鍵パリティ処理手段30-1と30-2の処理)

変数PATを64ビット長ブロックとし、その値は、そのビット位置の8, 16, 24, 32, 40, 48, 56, 64は0、その他のビット位置は全て1とする。即ち、

$PAT = \text{fefefefefefefefefe}$  (16進数表現)

とする。次に、入力した鍵の中のパリティビット有り/無を指定した場合に限り、 $KL = KL \oplus PAT$ 、 $KR = KR \oplus PAT$ とする。

(鍵処理拡張手段40の処理)

$KR$ を、2分割し、 $KR_0$ 、 $KR_1$ で表わす。即ち、 $KR = (KR_0, KR_1)$ とする。次に、32ビット長のブロック $U_0$ 、 $U_1$ 、 $U_2$ を次式で定める。

$$U_0 = KR_0 \oplus KR_1$$

$$U_1 = KR_0$$

$$U_2 = KR_1$$

(鍵処理部50の処理)

32ビット長のブロック $W_i$ 、 $i = 1, 2, 3, 4, 5, 6$ を次式で表わす。

$$W_0 = U_0$$

$$W_1 = U_1$$

$$W_2 = U_2$$

$$W_3 = U_0$$

$$W_4 = U_1$$

$$W_5 = U_2$$

する。

暗号化を指定した場合は、 $P_i$ は次の順序で信号線206から出力する。

$$P_4, P_5, P_6, P_7,$$

$$P_8, P_1, P_2, P_3,$$

$$P_9, P_0, P_{10}, P_{11}$$

復号を指定した場合は、 $P_i$ は次の順序で信号線206から出力する。

$$P_9, P_0, P_{10}, P_{11},$$

$$P_3, P_2, P_1, P_0,$$

$$P_4, P_5, P_6, P_7$$

(データランダム化部60)

(暗号化指定の場合)

平文ブロックの左右それぞれ4バイトのブロックを $L_0$ 、 $R_0$ として、まず

$$(L_0, R_0) = (L_0, R_0) \oplus (P_4, P_5, P_6, P_7)$$

$$(L_0, R_0) = (L_0, R_0) \oplus (\emptyset, L_0)$$

続いて、 $r = 1 \sim 4$ について、 $R_r$ と $L_r$ を逐次計算する。

$$R_r = L_{r-1} \oplus f(R_{r-1}, P_{r-1})$$

(5)

$A_r$ 、 $B_r$ 、 $D_r$ は、32ビット長ブロックを表わす変数とする。 $\emptyset$ は、全ビットが0の32ビット長ブロックを表わす。 $KL$ を2分割し、左半分を $A_0$ と右半分 $B_0$ とする、即ち、 $KL = (A_0, B_0)$ とする。

最初に、 $D_0 = \emptyset$ 、

$r = 1 \sim 6$ について、 $P_i$  ( $i = 0 \sim 11$ )を定める。

$$D_r = A_{r-1}$$

$$A_r = B_{r-1}$$

$$B_r = f_k(A_{r-1}, B_{r-1} \oplus D_{r-1} \oplus W_{r-1})$$

$$P_z(r-1) = B_{r1}$$

$$P_z(r-1)+1 = B_{rr}$$

ここで、 $B_{r1}$ は $B_r$ の左半分、 $B_{rr}$ は $B_r$ の右半分を表わし、 $B_r = (B_{r1}, B_{rr})$ である。関数 $f_k(\alpha, \beta)$ は、32ビット長ブロックの $\alpha$ と $\beta$ を入力してその各ビットをかき混ぜる処理(データ拡散)を行い、その結果を32ビット長ブロックとして出力する関数であり、例えば、特願昭62-37231の第7図に示されるデータ拡散手段を使って実現

$$L_r = R_{r-1}$$

次に、 $R_4$ 、 $L_4$ に対して

$$(R_4, L_4) = (R_4, L_4) \oplus (\emptyset, R_4)$$

$$(R_4, L_4) = (R_4, L_4) \oplus (P_9, P_0, P_{10}, P_{11})$$

暗号文ブロックは $(R_4, L_4)$ で得られる。

ここで、関数 $f$ は $(\alpha, \beta)$ は、32ビット長ブロックの $\alpha$ と16ビット長のブロック $\beta$ を入力してその各ビットをかき混ぜる処理(データ拡散)を行い、その結果を32ビット長ブロックとして出力する関数であり、例えば、特願昭62-37231の第5図に示されるデータ拡散手段を使って実現する。

(復号指定の場合)

暗号文ブロックの左右それぞれ4バイトのブロックを $R_4$ 、 $L_4$ として、まず、

$$(R_4, L_4) = (R_4, L_4) \oplus (P_9, P_0, P_{10}, P_{11})$$

$$(R_4, L_4) = (R_4, L_4) \oplus (\emptyset, R_4)$$

続いて、 $r = 4 \sim 1$ について、 $L_{r-1}$ と $R_{r-1}$ を逐次計算する。

$$L_{r-1} = R_r \oplus f(L_r, P_{r-1})$$

(6)

$$R_{r-1} = L_r$$

最後に、 $L_a, R_a$  に対して

$$(L_a, R_a) = (L_a, R_a) \oplus (\phi, L_a)$$

$$(L_a, R_a) = (L_a, R_a) \oplus (P_s, P_s, P_s, P_r)$$

平文ブロックは、 $(L_a, R_a)$  で得られる。

### 「実施例 2」

この発明による暗号装置の他の実施例は、実施例 1 から、鍵バリティ処理手段 30-1 と 30-2、及び入力部 101 と出力部 106 を省いたものである。信号線 200 は信号線 203 に接続し、信号線 202 は信号線 204 へ接続する。実施例 2 の動作は、実施例 1 の動作で鍵バリティ処理手段 30-1 と 30-2 の動作を省いたものに等しい。

### 「実施例 3」

この発明による暗号装置の更に他の実施例は、実施例 1 から、鍵ブロック分割手段 20、鍵バリティ処理手段 30-2 と鍵処理拡張手段 40 を省いたものである。ここで、入力部 103 は、信号線 203 へ接続する。信号線 205 へは、0 を、即ち、 $U_0 = 0, U_1 = 0, U_3 = 0$  を入力する。実施

例 3 の動作は、実施例 1 の動作で、鍵ブロック長 = 64 ビットを指定したときの動作に等しい。

### 「発明の効果」

以上述べたように構成されているから、鍵長が  $N$  ビットの暗号化復号手段から、鍵長が  $2N$  ビットの暗号装置が容易に実現できる。

### 4. 図面の簡単な説明

第 1 図はこの発明の一実施例を示すブロック図、第 2 図は鍵バリティ処理手段を示すブロック図、第 3 図は零設定制御部を示すブロック図、第 4 図は鍵処理拡張手段を示すブロック図、第 5 図は鍵処理部を示すブロック図、第 6 図はデータランダム化部を示すブロック図である。

特許出願人

日本電信電話株式会社

代理人

草野 卓

図 1

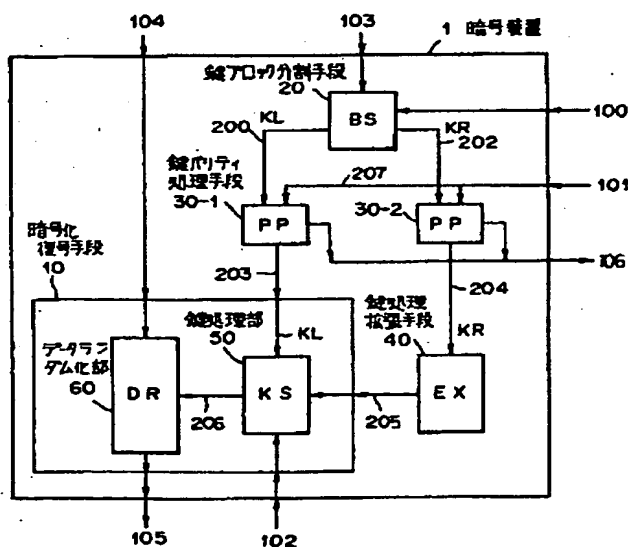


図 3

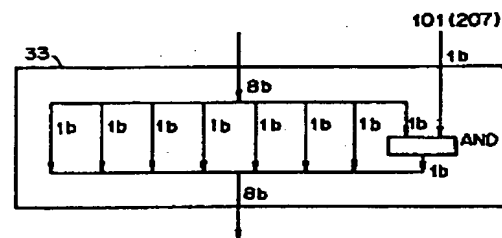
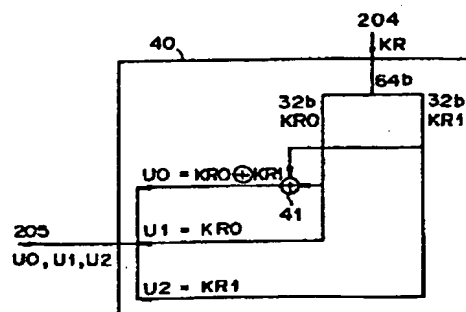


図 4







(8)

図 6

